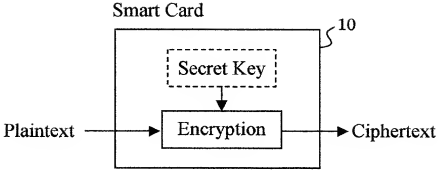


FIG. 1

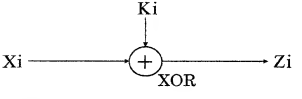


FIG. 2

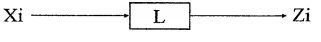


FIG. 3

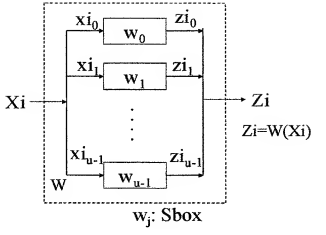


FIG. 4

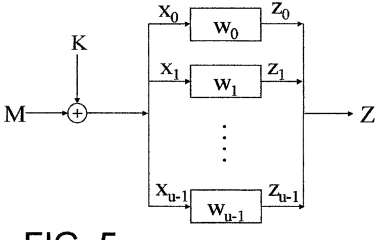


FIG. 5

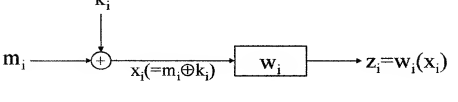


FIG. 6

FIG.7A

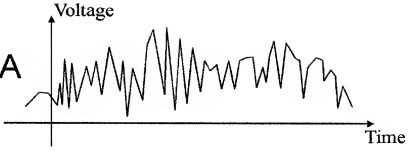


FIG.7B

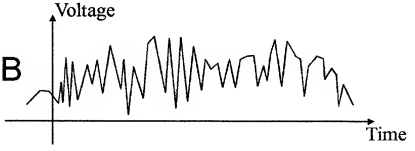


FIG.7C

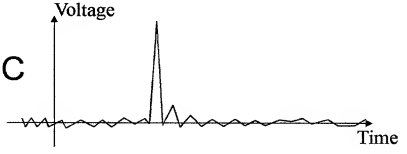
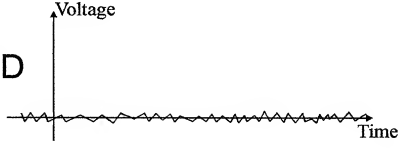


FIG.7D



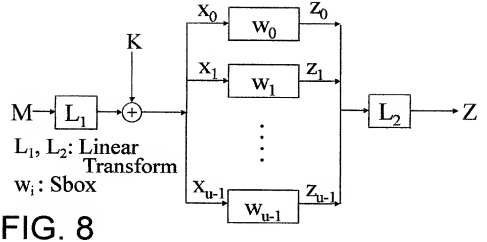


FIG. 8

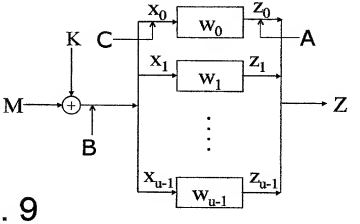


FIG. 9

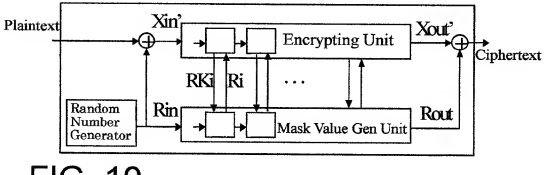
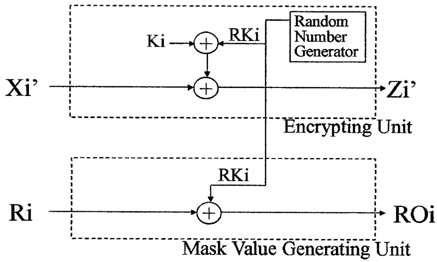


FIG. 10



Key XOR in Random Mask Value Method

FIG. 11

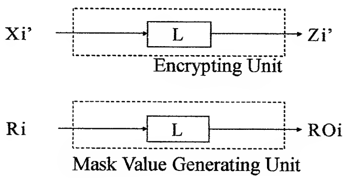


FIG. 12

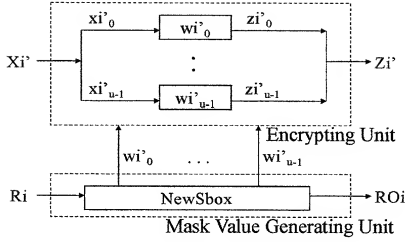


FIG. 13A

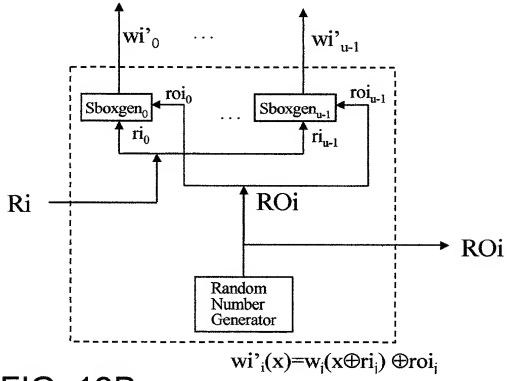
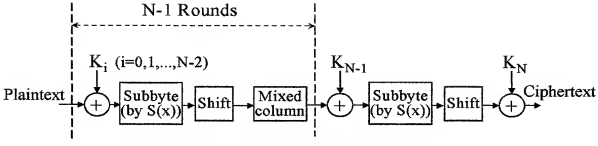
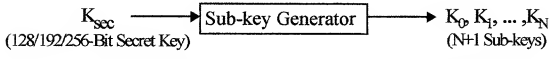


FIG. 13B



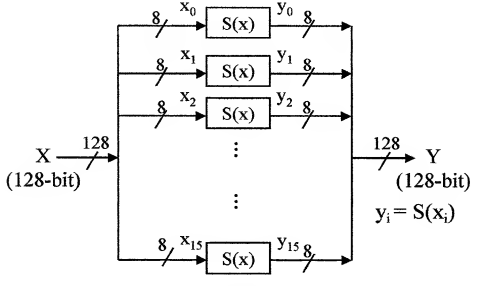
Conventional Rijndael Encryption

FIG. 14



Generation of Sub-keys in Rijndael Encryption

FIG. 15



Subbyte

FIG. 16

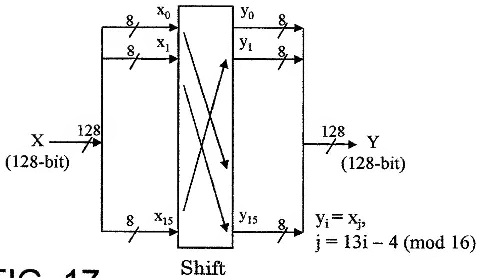
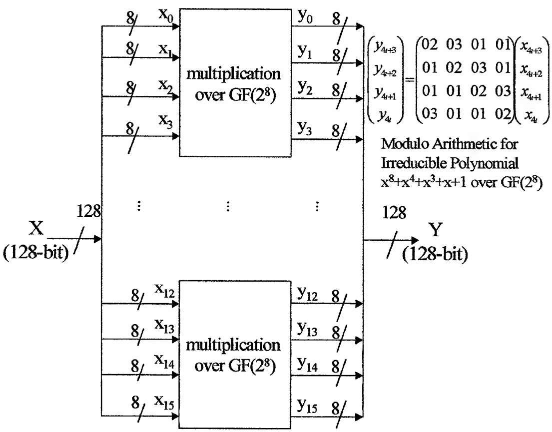


FIG. 17



$$\begin{pmatrix} y_{4i+3} \\ y_{4i+2} \\ y_{4i+1} \\ y_{4i} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} x_{4i+3} \\ x_{4i+2} \\ x_{4i+1} \\ x_{4i} \end{pmatrix}$$

FIG. 18

Mixedcolumn

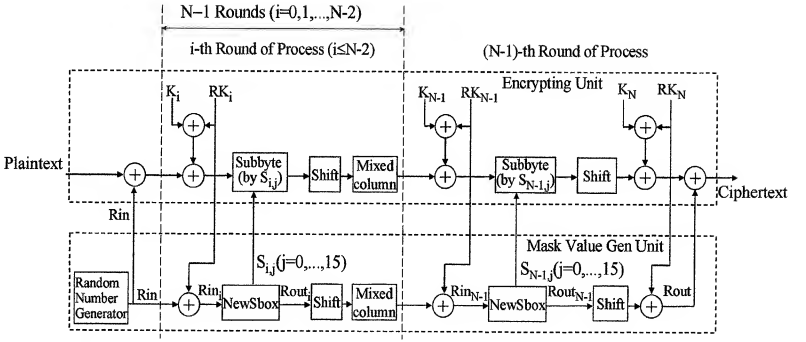
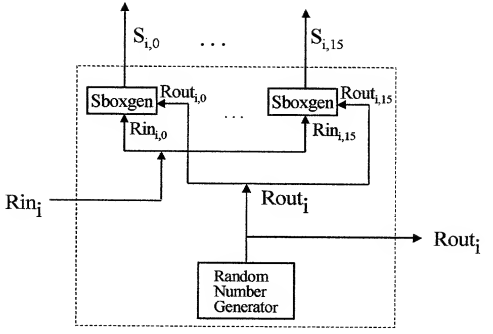


FIG. 19



Sboxgen Generates Sbox, $S_{i,j}$, such that $S_{i,j}(x)=S(x \oplus Rin_{i,j}) \oplus Rout_{i,j}$

NewSbox

FIG. 20

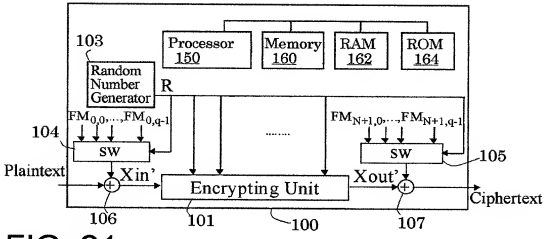


FIG. 21

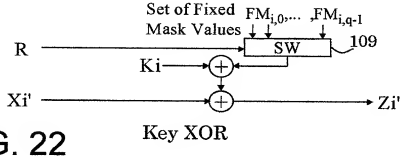


FIG. 22 Key XOR

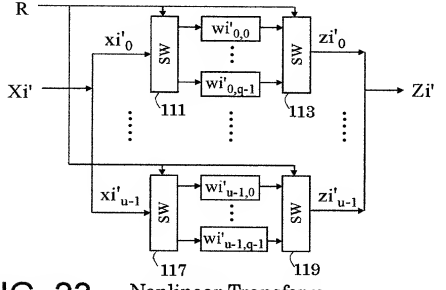


FIG. 23 Nonlinear Transform

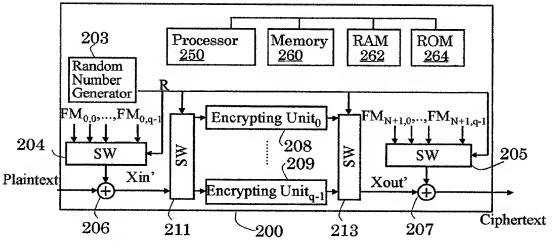


FIG. 24

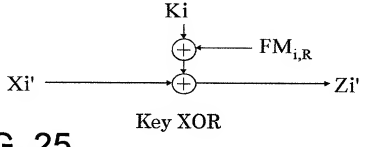


FIG. 25

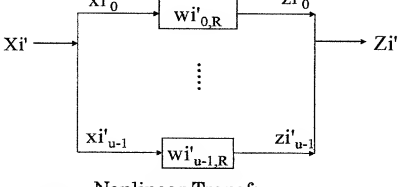


FIG. 26

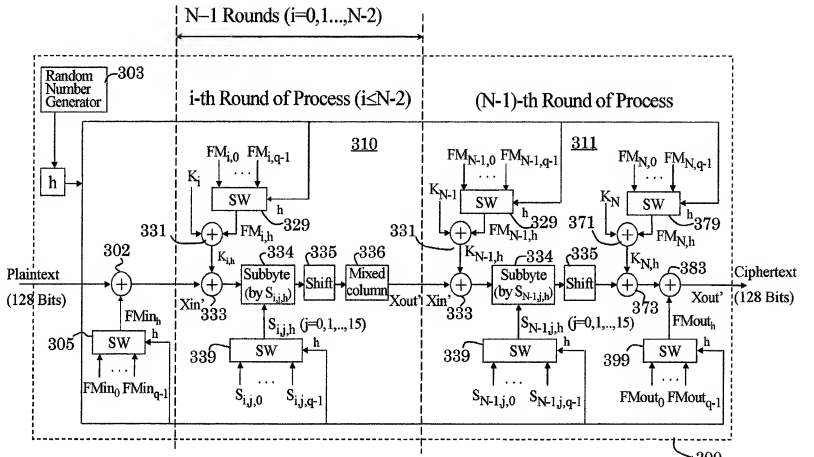
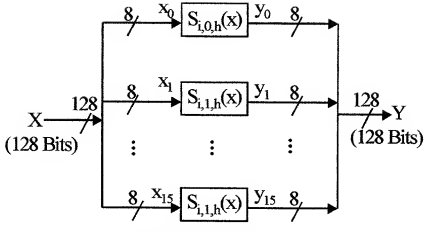


FIG. 27



$S_{i,j,h}(x)=S(x \oplus c_{i,j,h}) \oplus d_{i,j,h}$

S(x): Sbox in Conventional Rijndael Process

Subbyte

FIG. 28

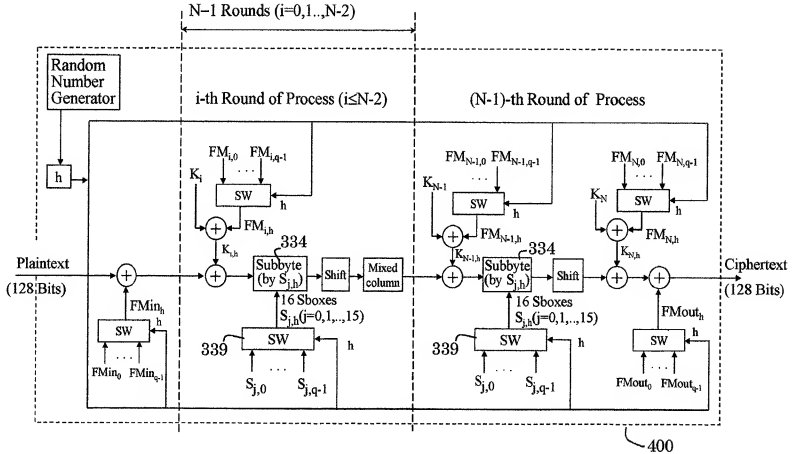


FIG. 29

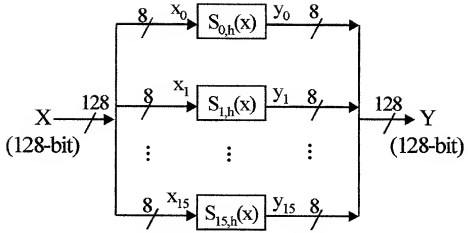

8
x_0
$S_{0,h}(x)$
y_0
8
x_1
$S_{1,h}(x)$
y_1
x_{15}
$S_{15,h}(x)$
y_{15}
128
X
(128-bit)
128
Y
(128-bit)
$S_{j,h}(x)=S(x\oplus c_{h,j})\oplus d_{h,j}$ (j=0,..,15)
(S(x): Sbox in Conventional Rijndael Process)
Subbyte

FIG. 30

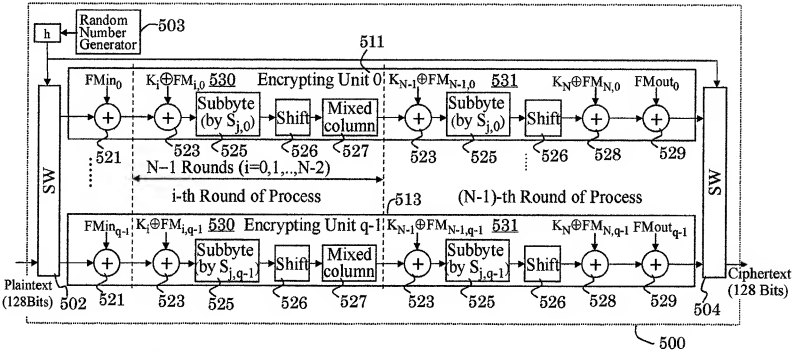


FIG. 31

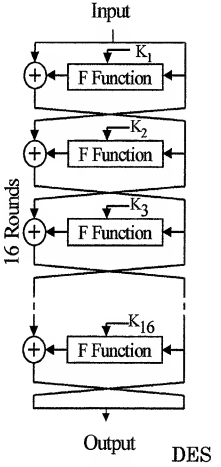


FIG. 32A

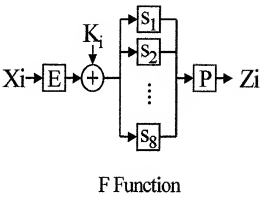


FIG. 32B

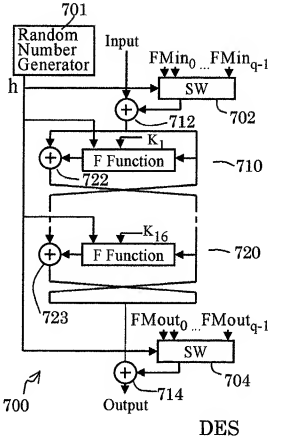
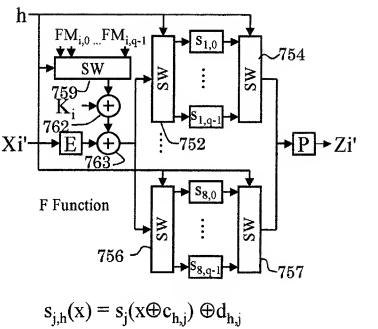


FIG. 33A



$$s_{j,h}(x) = s_j(x \oplus c_{h,j}) \oplus d_{h,j}$$

FIG. 33B

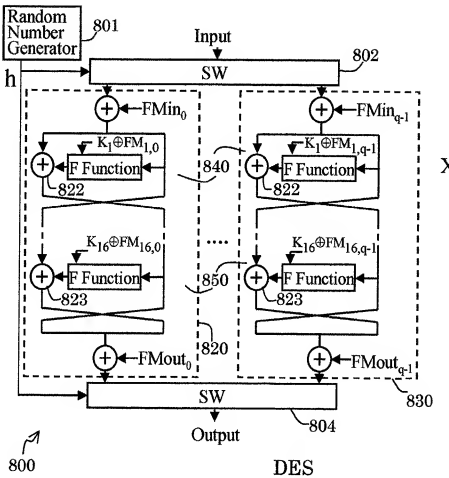


FIG. 34A

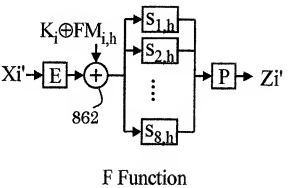
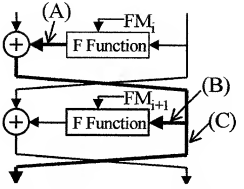
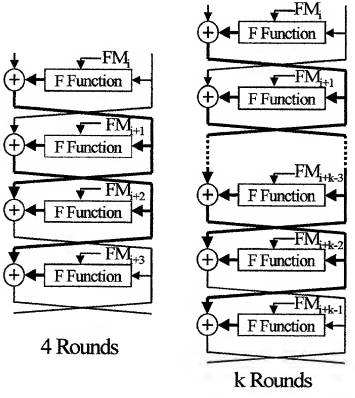


FIG. 34B



Propagation of Mask in Feistel Encryption

FIG. 35



Paths from Mask Value Generation to Cancellation in Feistel Encryption Device

FIG. 36